EXHIBIT 1
FILED UNDER SEAL - REDACTED VERSION OF DOCUMENT SOUGHT TO BE SEALED

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

FORTINET, INC., a corporation, Plaintiff, vs. SOPHOS, INC., a corporation, MICHAEL VALENTINE, an individual, and JASON CLARK, an individual, Defendants.	CASE NO. 3:13-cv-05831-EMC
SOPHOS, INC. and SOPHOS LTD., corporations, Counterclaim Plaintiffs, vs. FORTINET, INC., a corporation, Counterclaim Defendants.	**CONTAINS SOPHOS HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY AND HIGHLY CONFIDENTIAL – SOURCE CODE INFORMATION**

EXPERT REPORT OF DR. ANGELOS STAVROU REGARDING INFRINGEMENT OF U.S. PATENT NOS. 7,698,744, 8,069,487, 8,195,938, 7,376,125, AND 7,333,430

TABLE OF CONTENTS

I. INTRODUCTION 1

II. QUALIFICATIONS AND BACKGROUND 2

III. RETENTION AND COMPENSATION 10

IV. BASES FOR OPINION AND MATERIALS CONSIDERED 10

V. LEGAL STANDARDS 10

A. Infringement 11

B. Doctrine of Equivalents 11

C. Indirect Infringement 12

D. Person of Ordinary Skill in the Art 13

E. Legal Standard for Claim Construction 13

F. Legal Standard for Priority Date 18

VI. SUMMARY OF OPINIONS 18

VII. LEVEL OF ORDINARY SKILL IN THE ART 20

VIII. TECHNOLOGY BACKGROUND 20

A. Antivirus software 21

B. Kernel Mode and User Mode 22

C. Hashing 23

D. Network routing 24

IX. THE FORTINET PATENTS 25

A. The '744/'487/'938 patents 25

1. The asserted patents 25

2. The Architecture of the '744/'487/'938 Patents 26

3. Priority Date of the '744/'487/'938 Patents 28

B. The ‘430 patent 29
C. The ‘125 patent 30
X. OPERATIVE CLAIM CONSTRUCTIONS 31
XI. OPERATION OF THE ACCUSED PRODUCTS 33
A. The Endpoint Products 33
1. On-Access Driver 33
2. Antivirus Engine (SAVI) 44
3. Live Protection/SophosLabs 54
4. Sophos Cloud 55
5. Variations Between Versions 56
B. The UTM Products 57
XII. DIRECT INFRINGEMENT 59
A. Construed Claim Terms—Multi-Level Whitelisting Patents 60
1. “Whitelist” 60
2. “Local Whitelist” 62
3. “Global Whitelist” 62
4. “Multi-Level Whitelist” 63
5. “Trusted Third Party Service Provider” and “Trusted Service Provider” 63
6. “Cryptographic Hash Value” 64
B. The ‘744 patent 66
1. Claim 1 66
2. Claim 8 82
3. Claim 14 97
4. Claim 23 97
5. Claim 37 114

6. Sophos's Non-Infringement Contentions Regarding the '744 Patent.....128

C. The '487 patent 130

1. Claim 1.....130

2. Claim 7.....153

3. Claim 11.....159

4. Claim 13.....186

5. Claim 16.....187

6. Sophos's Non-Infringement Contentions Regarding the '487 Patent.....212

D. The '938 patent 215

1. Claim 1.....215

2. Claim 11.....241

3. Claim 15.....280

4. Claim 16.....286

5. Claim 18.....315

6. Sophos's Non-Infringement Contentions Regarding the '938 Patent.....315

E. The '125 patent 318

1. Construed Claim Terms 318

2. Claim 1.....319

3. Claim 2.....328

4. Claim 3.....329

5. Claim 4.....339

6. Claim 5.....340

7. Sophos's Non-Infringement Contentions Regarding the '125 Patent.....353

F. The '430 patent 354

1. Claim 1.....354

2. Claim 5 360

3. Claim 9 361

4. Claim 14 362

5. Claim 15 369

6. Sophos's Non-Infringement Contentions Regarding the '430 Patent 376

XIII. INDIRECT INFRINGEMENT 376

A. Induced Infringement 377

1. Sophos Customers Directly Infringe 377

2. Sophos Had Knowledge of the Fortinet Patents 379

3. Sophos Encourages and Instructs its Customers to Infringe 380

B. Contributory Infringement 382

1. The Accused Endpoint Products are a Material Part of the Invention 382

2. Sophos Knew that the Accused Endpoint Products were Especially Made or Especially Adapted for use in the Infringement of the '744, '487, and '938 Patents 383

3. The Accused Endpoint Products have no Substantial Non-Infringing Uses 383

I. INTRODUCTION

1. My name is Angelos Stavrou. I have been retained to testify as an expert in this action on behalf of Fortinet, Inc. For this report, I have been asked to provide analysis and expert opinions on the following topics: (a) the disclosures of U.S. Patent No. 7,698,744 ("the '744 patent"), U.S. Patent No. 8,069,487 ("the '487 patent"), U.S. Patent No. 8,195,938 ("the '938 patent"), U.S. Patent No. 7,376,125 ("the '125 patent"), and U.S. Patent No. 7,333,430 ("the '430 patent"); and (b) Sophos's infringement of all asserted claims of these patents (the "asserted claims").

2. My opinions and the bases for those opinions are contained in this expert report.

3. I expect to be called to provide expert testimony regarding opinions formed resulting from my analysis of the issues considered in this report if asked about those issues by the court or by the parties' attorneys. If asked to do so, I may also provide testimony describing computer security and networking, and the history of computer security and networking. I may also discuss my own work, teaching, and publications in the field, and knowledge of the state of the art in the relevant time period. I may rely on handbooks, textbooks, technical literature, my own personal experience in the field, and other relevant materials and/or information to demonstrate the state of the art in the relevant period and the evolution of relevant technologies. I may also provide testimony on any matters addressed by any expert testifying on behalf of Sophos, if asked about these matters by the Court or counsel for the parties. I may also provide testimony on any additional matters discussed herein.

4. I reserve the right to modify or supplement my opinions, as well as the basis for my opinions, in light of any documents, testimony, or other evidence that may emerge during the course of this matter, including additional deposition testimony or newly-produced documents.

5. In connection with my anticipated testimony in this action, I may use as exhibits various documents produced in this case that refer or relate to the matters discussed in this report. I have not yet selected the particular exhibits that might be used. In addition, I may create or assist in the creation of certain demonstrative evidence to assist me in testifying, and I reserve the right to do so, such as working computer systems or code highlighting to further support the positions in this report. For example, at trial I may rely on programs cited in this report, or compiled versions of related source code, or compiled versions of software programs discussed in this report, in order to illustrate the relevant functionality of that software and aide the jury in their understanding of this software.

6. It is also my understanding that Sophos may submit an expert report responding to this report. I reserve the right to rebut any positions taken in that report.

II. QUALIFICATIONS AND BACKGROUND

7. I summarize my qualifications for forming the opinions set forth in this expert report below. Those qualifications are described in more detail in my cv attached as Exhibit A. In short, I am an expert in the fields of computer security and networking.

8. I am an Associate Professor at George Mason University and the Director of the Center for Assurance Research and Engineering (CARE) at GMU. I am currently the Academic Director of two graduate-level programs at GMU the M.S. in Information Security and Assurance at the Computer Science Department and the M.S. in Management of Secure Information Systems Program, at the School of Management. The latter is one of the first inter-disciplinary programs that attempt to combine cyber security and management skills. I have served as principal investigator on research grants and contracts from NSF, DARPA, IARPA, DHS, AFOSR, ARO, ONR, and I am an active member of NIST's Mobile Security team. I have written more than 80 peer-reviewed conference and journal articles. I received my M.Sc. in

Electrical Engineering, M.Phil. and Ph.D. (with distinction) in Computer Science all from Columbia University. I also hold an M.Sc. in theoretical Computer Science from University of Athens, and a B.Sc. in Physics with distinction from University of Patras, Greece. My current research interests include security and reliability for distributed systems, security principles for virtualization, and anonymity with a focus on building and deploying large-scale systems.

9. Over the past several years, my research has focused on two aspects of security: Systems' Security and Reliability. In the context both of this research goals, I worked alongside with researchers from National Institute of Standards and Technology (NIST) as part of the DARPA "Transformative Apps" (TransApps) effort that aimed to secure Android mobile phone devices against a wide range of attacks. As part of my research with NIST under the auspices of the DARPA "Transformative Apps" project, we designed and implemented the AppVet [1] framework which has been used as an operational system to securely deploy thousands of commercial smartphones in the battlefield: in 2011, as part of this effort, we delivered a batch of commercially available smartphones and an initial set of secure, soldier-defined apps to an Army brigade in Afghanistan. By 2013, about 4,000 mobile devices (smartphones and tablets) were deployed in Afghanistan, and an online application store was up and running for soldiers[2].

10. For our efforts, National Institute of Standards and Technology (NIST) researchers have earned a 2014 *GCN* Award for Information Technology Excellence [3] for speeding development and delivery of secure, battlefield-handy—and sometimes lifesaving—smartphone apps to U.S. troops in Afghanistan.

---

[1] http://csrc.nist.gov/projects/appvet/

[2] http://www.nist.gov/el/isd/transapp-090314.cfm

[3] http://gcn.com/Articles/2014/08/18/2014-GCN-Award-Winners.aspx?Page=3

11. Moreover, DARPA's TransApps program has earned high marks from its customers and prompted testimonials from the battlefield. Here's an example: "The Taliban had nearly surrounded us. We used the handheld (TransApps device) to identify the enemy's position and fired directly at them. If we would not have had the device to pinpoint the enemy, lives could have been lost." Besides Afghanistan, TransApp devices were used by police and others at the 2013 presidential inauguration and at the 2014 Boston Marathon[4].

12. AppVet's security architecture lets the government keep pace with the fast-paced mobile industry while adhering to strict security requirements, replacing the costly model of long development times and government-specific solutions. In addition, we produced a meaningful reference implementation for the private sector that can help in the development of secure devices and applications. This can help agencies solve problems associated with the bring-your-own-device movement, which can introduce unmanaged and untrusted personal devices into the government workplace.

13. AppVet is a framework that introduces software assurance methodology, power and reliability analysis techniques, and standards-based cryptographic solutions using a simple, open-source web service for vetting mobile applications. AppVet facilitates the mobile application vetting workflow by providing an intuitive user interface for submitting and testing applications, accessing reports, and assessing risk. Through the specification of simple APIs and requirements, AppVet is designed to easily and seamlessly integrate with a wide variety of clients including application stores and continuous integration environments as well as third-party analysis tools including static and dynamic analyzers, anti-virus scanners, and vulnerability repositories. AppVet can support analysis of applications from different platforms so long as

[4] http://www.nist.gov/el/isd/transapp-090314.cfm

there are tools available to analyze those applications. AppVet takes a simple approach to deriving an application's risk assessment based on the risk assessments from multiple tools. If an application receives low-risk assessments from all tools, then AppVet assigns an overall risk assessment of PASS (low-risk). If an application receives a high-risk assessment from at least one tool, then AppVet assigns an overall risk assessment of FAIL (high-risk). If an application receives a moderate-risk assessment from at least one tool, but does not receive any high-risk assessments, AppVet assigns an overall risk assessment of WARNING (moderate-risk).

14. Furthermore, I was the GMU PI participating in the IARPA Securely Taking On New Executable Software of Uncertain Provenance (STONESOUP)[5] effort. STONESOUP aimed to develop and demonstrate comprehensive, automated techniques that allow end users to securely execute software without basing risk mitigations on characteristics of provenance that have a dubious relationship to security. Existing techniques to find and remove software vulnerabilities are costly, labor-intensive, and time-consuming. Many risk management decisions are therefore based on qualitative and subjective assessments of the software suppliers' trustworthiness.

15. The goal of the STONESOUP program was to develop and demonstrate technology that provides comprehensive, automated techniques that allow end users to safely execute new software of uncertain provenance. The envisioned technology will use advanced automated software analysis techniques to identify vulnerabilities or to assure their absence; it will combine the analysis with methods for confining software execution so that identified weaknesses cannot be exploited; and it will diversify software components so any residual vulnerabilities will be more difficult for attackers to discover or exploit. The combination of

[5] http://www.iarpa.gov/index.php/research-programs/stonesoup

these techniques can provide true defense-in-depth against attempts to exploit vulnerable software.

16. As part of a team, we designed and build MINESTRONE, a versatile architecture that incorporates a number of component technologies using a combination of analysis, confinement, and diversification approaches. MINESTRONE leverages confinement to mitigate potential vulnerabilities and can be deployed to transparently protect running applications using dynamic security instrumentation.

17. MINESTRONE is a novel architecture that integrates static analysis, dynamic confinement, and code diversification techniques to enable the identification, mitigation and containment of a large class of software vulnerabilities. Our techniques protect new software, as well as already deployed (legacy) software by transparently inserting extensive security instrumentation. They also leverage concurrent program analysis (potentially aided by runtime data gleaned from profiling software) to gradually reduce the performance cost of the instrumentation by allowing selective removal or refinement.

18. MINESTRONE employs diversification techniques for confinement and fault-tolerance purposes. To minimize performance impact, our project will also leverage multi-core hardware or (when unavailable) remote servers to enable the quick identification of potential compromises. The developed techniques require no specific hardware or operating system features, although they will take advantage of such features where available, to improve both runtime performance and vulnerability coverage.

19. In addition, I was funded by DARPA under the Cyber Genome project to perform analysis on the phylogenetic origins of malware. The objective of the Cyber Genome Program was to produce revolutionary cyber defense and investigatory technologies for the collection,

identification, characterization, and presentation of properties and relationships from collected digital artifacts of software, data, and/or users to support DoD law enforcement, counter intelligence, and cyber defense teams. Digital artifacts may be collected from live systems (traditional computers, personal digital assistants, and/or distributed information systems such as 'cloud computers'), from wired or wireless networks, or collected storage media. The format may include electronic documents or software (to include malicious software - malware).

20. In the Cyber Genome project, I was part of a team that developed CyNomiX, a novel framework for scalable identifications of the lineage of malicious programs and threats. One of the tools we developed was PyTrigger, a dynamic malware analysis system that automatically exercises a malware binary extracting its behavioral profile even when specific user activity or input is required. To accomplish this, we developed a novel user activity record and playback framework and a new behavior extraction approach. Unlike existing research, the activity recording and playback includes the context of every object in addition to traditional keyboard and mouse actions. The addition of the context makes the playback more accurate and avoids dependencies and pitfalls that come with pure mouse and keyboard replay. Moreover, playback can become more efficient by condensing common activities into a single action. After playback, PyTrigger analyzes the system trace using a combination of multiple states and behavior differencing to accurately extract the malware behavior and user triggered behavior from the complete system trace log[6].I am currently the principal investigator on an NSF grant on "Scalable Techniques for Better Situational Awareness: Algorithmic Frameworks and Large-

[6] Dan Fleck, Arnur G. Tokhtabayev, Alex Alarif, Angelos Stavrou, Tomas Nykodym: PyTrigger: A System to Trigger & Extract User-Activated Malware Behavior. ARES 2013: 92-101.

Scale Empirical Analyses"[7]. This project involves researchers from George Mason University and University of North Carolina at Chapel Hill and aims to further our collective understanding of the growing abuse of enterprise name servers whereby infected clients (bots) use automated domain-name generation algorithms to bypass network defenses. More specifically, a framework for accurately identifying bots upon seeing only a handful of unique lookups is developed based on sequential hypothesis testing. The integration of NetFlow records, with novel their indexing data-structures, delivers even deeper insight into aberrant traffic. A live deployment of the system demonstrates the utility of this approach and provides the opportunity for interactively querying the recorded forensic information.

21. Another NSF project I am the principal investigator for is the NSF 1303299[8], on "Bridging the Cybersecurity Leadership Gap: Assessment, Competencies and Capacity Building". This effort seeks to foster cross-disciplinary education as a foundation for the development and assessment of cybersecurity leadership education programs. In addition, my research team is currently funded by DARPA under the Active Authentication, and Mission Resilient Cloud projects. Furthermore, we are current involved in funded projects from ADD and DHS for research efforts in security mobile and IoT devices.

22. Some relevant publications include:

- **NetGator: Malware Detection Using Program Interactive Challenges.** Brian Schulte, Haris Andrianakis, Kun Sun, Angelos Stavrou: In the proceedings of DIMVA 2012: 164-183.

[7] http://www.nsf.gov/awardsearch/showAward?AWD_ID=1421747

[8] http://www.nsf.gov/awardsearch/showAward?AWD_ID=1303299

- **Malware Characterization Using Behavioral Components.** Chaitanya Yavvari, Arnur G. Tokhtabayev, Huzefa Rangwala, Angelos Stavrou. In the proceedings of MMM-ACNS 2012: 226-239.
- **PyTrigger: A System to Trigger & Extract User-Activated Malware Behavior.** Dan Fleck, Arnur G. Tokhtabayev, Alex Alarif, Angelos Stavrou, Tomas Nykodym. In the proceedings of ARES 2013: 92-101.
- **Using Hardware Features for Increased Debugging Transparency.** Fengwei Zhang, Kevin Leach, Angelos Stavrou, Haining Wang, and Kun Sun. In the Proceedings of the 36th IEEE Symposium on Security and Privacy (Oakland 2015), San Jose, CA, May 2015.
- **On the Infeasibility of Modeling Polymorphic Shellcode: Re-thinking the Role of Learning in Intrusion Detection Systems**. Yingbo Song, Michael E. Locasto, Angelos Stavrou, Angelos D. Keromytis, and Salvatore J. Stolfo. In the Proceedings of Machine Learning Journal (MLJ) p. 179-205. Accepted: 7 August 2009, Published online: 29 October 2009.

23. I was awarded with the 2012 George Mason Emerging Researcher, Scholar, Creator Award[9], a university-wide award. In 2013, I received the IEEE Reliability Society Engineer of the Year award that recognizes outstanding contributions to the Reliability discipline within the last few years[10].

24. I am a NIST guest researcher and a senior IEEE member. I am also a member of the ACM and USENIX.

[9] http://research.gmu.edu/grants_awards.html

[10] http://rs.ieee.org/awards.html#engineer

III. RETENTION AND COMPENSATION

25. I am being compensated for my work on this case at my standard consulting rate of $350 per hour except for time spent testifying at deposition or trial, for which I charge $450 per hour. I am also being reimbursed for expenses that I incur. My compensation is not contingent upon the results of my analysis or the substance of my testimony.

IV. BASES FOR OPINION AND MATERIALS CONSIDERED

26. In preparing this report, I have reviewed the asserted Fortinet patents including their claims, specifications, and drawings, as well as their prosecution histories. I have reviewed public and publicly available and internal documentation maintained by Sophos relating to the accused products including, e.g., manuals, requirements documents, specifications, and design documents. I have also reviewed source code for the accused products. I personally inspected source code for the accused products for five days, and also reviewed printouts of source code that I understand were requested by Fortinet. Exemplary citations to those materials are included throughout this expert report. A list of materials I have considered in reaching the conclusions described in this expert report is contained in Exhibit B. I may rely on those materials, as well as any additional materials cited in sections of my expert report in support of my opinions. I am also relying on my own education and technical experience.

V. LEGAL STANDARDS

27. I am not a lawyer. However, counsel for Fortinet has informed me of general guidelines and rules for examining the claims of a patent to determine whether or not a claim is infringed.

28. I understand that analyzing patent infringement generally involves two steps. First, the Court must construe any claim term for which the parties dispute the meaning or scope of the term. I understand that the Court has issued an Order which construes various claim terms

and sets forth the Court's constructions. Infringement is determined by comparing what is accused of infringement to the claims as construed by the Court.

29. My analyses apply the Court's claim constructions in this case. Where the Court has not construed a particular term I have applied the term as would be understood by a person of ordinary skill in the art of the particular patent at issue. In so doing, I considered the plain language of the claim in the context of the language of the other claims, the patent specification, and the prosecution history.

30. I understand that the second step in an infringement analysis is to compare an accused process or product with the asserted claim and that infringement may be established either literally or under the doctrine of equivalents.

A. Infringement

31. I understand that Fortinet has the burden to prove infringement. I have been informed that analysis of patent infringement requires two steps. The first step is to properly construe the patent claims, which is a step taken by the Court. The second step is to apply the construed claims to the accused product. A patent claim is "literally" infringed only if each and every claim element is found in the accused product.

B. Doctrine of Equivalents

32. I understand that, if not literally infringed, a patent claim might still be infringed under the "doctrine of equivalents." I am informed that pursuant to this doctrine if there are claim limitations that are not literally present in the accused product, the claim might still be infringed if the differences between the accused product and the claims are insubstantial for each claim limitation. I understand that one test used to determine whether differences are insubstantial is to determine whether a substitute element performs substantially the same

function in substantially the same way to obtain substantially the same result as the claimed element.

C. Indirect Infringement

33. I understand that direct infringement requires one party to perform or use each and every step or element of a claimed method or product. For method claims, direct infringement occurs when a single party performs all of the steps of the process.

34. I understand that where the actions of multiple parties combine to perform every step of a claimed method, the claim is directly infringed only if one party exercises control or direction over the entire process such that every step is attributable to the controlling party.

35. I understand that a person is liable for infringement of a patent by another if he or she actively induces the infringement. For example, a person may be found to have actively induced infringement if, knowing about a patent, she sells products that can be used to infringe the patent, and instructs her customers about how to perform actions that directly infringe the patent or otherwise helps the customers perform those actions, if she knew her actions would both cause the infringing acts of direct infringement, and that these acts would constitute patent infringement. I understand that a person who willfully blinds herself may be deemed to be actively inducing infringement if she actually believes that there is a high probability that her actions will induce actual infringement and she takes deliberate action to avoid learning whether her actions are inducing actual infringement.

36. I understand that contributory infringement requires a showing of direct infringement of the asserted claim by a single infringer. Contributory infringement also requires a showing that the accused devices have no substantial non-infringing uses, and that the alleged contributory infringer engaged in conduct within the United States that contributed to another's direct infringement in the United States.

of digital signatures.[35] The Whitecell provisional discloses that the Kernel Driver checks a file first against the "most recently used list of modules," then against a "Local Approved List" of digital signatures, and then against a "Global List" of digital signatures.[36] The Whitecell provisional states that the "Local Approved List" may be a "subset" of the global list.[37] The Whitecell provisional also states that the global list may be maintained by a "service provider."[38]

88. To the best of my knowledge, Sophos has not set forth any contention that the asserted claims are not entitled to the filing date of the Whitecell provisional. If they do so, I reserve the right to respond to that contention.

B. The '430 patent

89. The application that issued as the '430 patent was filed on July 6, 2005, and issued on February 29, 2008. It is titled "Systems and Methods for Passing Network Traffic Data."

90. The '430 patent generally describes methods of distributing the processing of network traffic among various "worker modules."[39] In disclosed embodiments, the disclosed system includes a pair of "IO modules" 102 and 104 that interface with senders and receivers of network traffic.[40] The IO modules receive network traffic and distribute that traffic to a worker module, such as worker modules 106a-106c, for processing.[41]

---

[35] FANTON000001 at FANTON000015-16.

[36] FANTON000001 at FANTON000015-16.

[37] FANTON000001 at FANTON000019.

[38] FANTON000001 at FANTON000018.

[39] '430 patent at Abstract,

[40] '430 patent at Fig. 1; 3:22-25.

[41] '430 patent at Fig. 1; 3:25-35.

91. The '430 patent discloses that "[v]arious distribution algorithms may be used to determining to which of the worker modules" to pass a packet.[42] For instance, the decision to which worker module to pass a packet may be "based on one or more IP addresses associated with the packet."[43] For instance, one of the sender or receiver IP addresses associated with the packet, or the some of those values, may be divided by a number N that represents the number of worker modules.[44] The remainder of that operation of that operation may be used to assign a packet to a worker module associated with that value.[45]

92. Once a worker module receives a packet, it can perform one or more of a number of different tasks, including "source verification, destination verification, user authentication, anti-virus, content scanning, content detection, intrusion detection, or other functions associated with policy enforcement."[46]

93. The IO modules and worker modules may tag packets to assist in routing of packets and communication of packet status.[47]

C. The '125 patent

94. The application that issued as the '125 patent was filed on June 4, 2002, and the '125 patent issued May 20, 2008. It is titled "Service Processing Switch."

95. Embodiments of the '125 patent relate to packet switching, and in particular, providing IP services in an integrated fashion.[48] It refers to the disclosed embodiment as an "IP Service Generator" or "IPSG."[49]

---

[42] '430 patent at 6:25-29.

[43] '430 patent at 6:26-29.

[44] '430 patent at 6:29-45.

[45] '430 patent at 6:45-62 (explaining an example of this process).

[46] '430 patent at 8:52-64.

[47] '430 patent at 4:40-5:11.

840. I will address these in turn. Sophos first argues that its products do not "establish a flow cache or a virtual router flow for established packet communications that is based on forwarding state information." But the "establishing" limitations of the claims do not require that establishing to be "based on forwarding state information." Sophos next argues that its products do not "have a virtual routing engine structure." The term "virtual routing engine structure" does not appear in the claims, and it is unclear what Sophos intends the term "structure" to mean in this context. "Virtual routing engine" does appear in the claims, and I explain how that limitation is met above. Finally, Sophos argues that its products do not "perform classify data packets based on flow." Again, it is not clear what Sophos means. Should Sophos substantiate or further explain any of its arguments, I reserve the right to rebut.

F. The '430 patent

841. Each of the accused UTM products, when sold, imported, or otherwise supplied by Sophos, and when used by Sophos or its customers, directly provides an practices the asserted claims of the '430 patent.

1. Claim 1

842. In my opinion, Sophos and its customers directly infringe this claim via operation of the accused products. Customers directly infringe when the accused products run in the United States. Sophos directly infringes by hosting instances of the accused UTM products [redacted] and by using the accused endpoint products internally within the United States.[1604]

(a) *A method for processing network traffic data, comprising: receiving network traffic data; and*

[redacted]

[1604] https://www.sophos.com/en-us/company/contact.aspx (referencing Sophos sites in Burlington, MA and Santa Clara, CA).

843. The accused UTM products receive network traffic data.

844. [redacted]

[1605] Stutz Tr. 71:2-14; 71:16-72:20; 73:14-23; 76:25-77:11; 78:7-80:8

[redacted]

[1607] Stutz Tr. 31:24-33:16

[1608] Stutz Tr. 25:15-26:2

[redacted]

(b) *passing the network traffic data to one of a plurality of worker modules for processing the network traffic data;*

848. The accused UTM products pass the network traffic data to one of a plurality of worker modules for processing the network traffic data. [redacted]

[redacted]

[1611] Stutz Tr. 57:17-58:17.

[redacted]

(c) *wherein the step of passing is performed based at least in part on a quantity of the worker modules; and*

849. The accused UTM products perform the passing step based at least in part on a quantity of the worker modules.

850. [redacted]

851. [redacted]

852. [redacted]

[1612] Stutz Tr. 46:3-47:16

[1613] See 4/22/2015 Stutz Tr. 25:15-26:2; [redacted].

[1614] [redacted]

[redacted]

853. [redacted]

[redacted]

854. [redacted]

[redacted]

[redacted]

[1616] Stutz Tr. 20:1-18.

[redacted]

[redacted]

(d) *wherein each of the worker modules has an identification number, and the network traffic data is passed based on a matching between a value and the identification number of one of the worker modules, the value obtained using at least an IP address associated with a receiver of the network traffic data.*

855. In the accused UTM products, each of the worker modules has an identification number, and the network traffic data is passed based on a matching between a value and the identification number of one of the worker modules, the value obtained using at least an IP address associated with a receiver of the network traffic data.

856. [redacted]

857. [redacted]

[redacted]

[redacted]

2. Claim 5

(a) *The method of claim 1, further comprising using the one of the plurality of worker modules to perform stateful inspection, intrusion detection, or antivirus.*

858. The accused UTM products use the one of the plurality of worker modules to perform stateful inspection, intrusion detection, or antivirus.

859. [redacted]

[redacted]

[1628] See 4/22/2015 Stutz Tr. 32:5-33:17.

[redacted]

3. Claim 9

(a) *The method of claim 1, further comprising tagging the network traffic data.*

860. The accused UTM products tag the network traffic data [redacted]

[redacted]

[1629] [redacted]

[1630] See 4/22/2015 Stutz Tr. 32:5-33:17.

[1631] [redacted]

[1632] http://people.netfilter.org/pablo/docs/login.pdf at page 35-39

[1633] http://people.netfilter.org/pablo/docs/login.pdf at page 35-39

[1634] http://www.tldp.org/HOWTO/Adv-Routing-HOWTO/lartc.netfilter.html

[1635] Stutz Tr. 71:2-72:19.

[redacted]

[redacted]

861. [redacted]

[redacted]

4. Claim 14

862. In my opinion, Sophos and its customers directly infringe this claim. Sophos directly infringes this claim by selling or importing in or into the United States the claimed system in the form of either appliances or software in the form CDs, digital downloads, or other distribution methods. Sophos also directly infringes by [redacted]. Sophos customers directly infringe through installation and use of the accused UTM products in the United States.

(a) *A system for processing network traffic data, comprising: means for receiving network traffic data; and*

863. The accused UTM products are each a system that includes a means for receiving network traffic data.

864. The term "means for receiving network traffic data" is written in means-plus-function form, and recites a function of "receiving network traffic data." Based on my review of

[redacted]

the specification of the '430 patent, I believe that the structure corresponding to that function is identified as communication interface 618.[1639] I note that the function and corresponding structure I propose is identical to Sophos's own.[1640]

865. [redacted]

866. If the Court later provides a different construction for "means for receiving," I reserve the right to supplement my opinions to address any new construction.

867. [redacted].

868. [redacted]

[1639] *See* Fig. 6.

[1640] Dkt. 80 (Joint Claim Construction Statement) at Appx. B, pg. 55.

[1641] *See, e.g.*, https://www.sophos.com/en-us/medialibrary/PDFs/factsheets/sophosutm525dsna.pdf?la=en (UTM 525) at 3.

[1642] Stutz Tr. 71:2-14; 71:16-72:20; 73:14-23; 76:25-77:11; 78:7-80:8 [redacted]

[redacted]

869. [redacted]

870. [redacted]

[1644] Stutz Tr. 31:24-33:16

[1645] Stutz Tr. 25:15-26:2

[redacted]

[1648] Stutz Tr. 57:17-58:17.

[redacted]

(b) *means for passing the network traffic data to one of a plurality of worker modules for processing the network traffic data;*

871. The accused UTM products are each a system that includes a means for passing the network traffic data to one of a plurality of worker modules for processing the network traffic data.

872. The term "means for passing the network traffic data to one of a plurality of worker modules for processing the network traffic data" is written in means-plus-function form, and recites a function of "passing the network traffic data to one of a plurality of worker modules for processing the network traffic data." Based on my review of the specification of the '430 patent, I believe that the structure corresponding to that function is identified as bus 602.[1649] I note that the function and corresponding structure I propose is identical to Sophos's own.[1650]

873. The accused UTM products include a communications bus. [redacted]

874. If the Court later provides a different construction for "means for passing," I reserve the right to supplement my opinions to address any new construction.

875. [redacted]

[1649] '430 patent at 14:47-15:13; 16:1-2.

[1650] Dkt. 80 (Joint Claim Construction Statement) at Appx. B, pg. 55.

[redacted]

(c) *wherein the means for passing is configured to perform the step of passing based at least in part on a quantity of the worker modules; and*

876. In the accused UTM products, the means for passing is configured to perform the step of passing based at least in part on a quantity of the worker modules.

877. [redacted]

878. [redacted]

[1651] Stutz Tr. 46:3-47:16

[1652] See 4/22/2015 Stutz Tr. 25:15-26:2; [redacted]

879. [redacted]

880. [redacted]

[redacted]

[1655] Stutz Tr. 20:1-18.

[redacted]

[redacted]

(d) *wherein each of the worker modules has an identification number, and the means for passing passes the network traffic data based on a matching between a value and the identification number of one of the worker modules, the value obtained using an IP address associated with a receiver of the network traffic data.*

882. In the accused UTM products, each of the worker modules has an identification number, and the means for passing passes the network traffic data based on a matching between a value and the identification number of one of the worker modules, the value obtained using an IP address associated with a receiver of the network traffic data.

883. [redacted]

[redacted]

884. [redacted]

5. Claim 15

885. In my opinion, Sophos and its customers directly infringe this claim. Sophos directly infringes this claim by selling or importing in or into the United States computer products having stored instructions, such as appliances or software in the form CDs, digital downloads, or other distribution methods. Sophos also directly infringes by [redacted]

[redacted]

[redacted]. Sophos customers directly infringe through installation and use of the accused UTM products in the United States.

(a) *A computer product having a set of stored instructions, an execution of which causes a process to be performed, the process comprising: receiving network traffic data; and*

886. The accused products include instructions that, when executed, receive network traffic data.

887. [redacted]

888. [redacted]

[redacted]

[1668] Stutz Tr. 71:2-14; 71:16-72:20; 73:14-23; 76:25-77:11; 78:7-80:8

[redacted]

[1670] Stutz Tr. 31:24-33:16

889. [redacted]

890. [redacted]

(b) *passing the network traffic data to one of a plurality of worker modules for processing the network traffic data;*

891. The accused products include instructions that, when executed, pass the network traffic data to one of a plurality of worker modules for processing the network traffic data.

[1671] Stutz Tr. 25:15-26:2

[redacted]

[1674] Stutz Tr. 57:17-58:17.

892. [redacted]

(c) *wherein the step of passing is performed based at least in part on a quantity of the worker modules; and*

893. The accused products include instructions that, when executed, perform the step of pass is performed based at least in part on a quantity of the worker modules.

894. [redacted]

895. [redacted]

[1675] Stutz Tr. 46:3-47:16

[1676] See 4/22/2015 Stutz Tr. 25:15-26:2; [redacted]

[redacted]

896. [redacted]

[redacted]

897. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[1679] Stutz Tr. 20:1-18.

[redacted]

[redacted]

898. [redacted]

[redacted]

(d) *wherein each of the worker modules has an identification number, and the network traffic data is passed based on a matching between a value and the identification number of one of the worker modules, the value obtained using an IP address associated with a receiver of the network traffic data.*

899. The accused products include instructions that, wherein each of the worker modules has an identification number, and the network traffic data is passed based on a matching between a value and the identification number of one of the worker modules, the value obtained using an IP address associated with a receiver of the network traffic data.

900. [redacted]

[redacted]

[redacted]

901. [redacted]

[redacted]

[redacted]

6. Sophos's Non-Infringement Contentions Regarding the '430 Patent

902. Sophos, in its contentions regarding why it does not practice the invention of the '430 patent, largely merely parrots the claim language.[1691] Its additional arguments also does little more than parrot language from the claims, without evidence or analysis:

> For example, Fortinet's Infringement Contentions do not establish that the accused Sophos products route network traffic based on the quantity of worker modules, nor that the Sophos accused products use an identification number that is separate from a device's internet address. Similarly, Fortinet's Infringement Contentions do not establish that Sophos's accused products tag network data. [1692]

903. I will address these in turn. Sophos first argues that its products do not "route network traffic based on the quantity of worker modules, nor that the Sophos accused products use an identification number that is separate from a device's internet address." But as I discuss above, flows are assigned to worker modules based on the number of worker modules, and the conntrack cache uses a node ID that is not the IP address. Sophos next argues that its products do not "tag network data." But as discussed above, the warp protocol employed by the accused UTM products tag incoming packets to route the packets to the destination worker module. Should Sophos substantiate or further explain any of its arguments, I reserve the right to rebut.

XIII. INDIRECT INFRINGEMENT

904. I have discussed above the direct infringement of the Fortinet patents in the previous sections of this report. In this section, I discuss my conclusion that Sophos not only directly infringes, but also indirectly infringes, via both induced and contributory infringement,

---

[1691] Sophos Inc. and Sophos LTD.'S Supplemental Responses to Interrogatories Propounded by Fortinet, Inc. (Interrogatory Nos. 1-5, 10, 19, 21-22) at 3-4.

[1692] Sophos Inc. and Sophos LTD.'S Supplemental Responses to Interrogatories Propounded by Fortinet, Inc. (Interrogatory Nos. 1-5, 10, 19, 21-22) at 4.

Date: July 20, 2015

Dr. Angelos Stavrou